



*SPI : une infrastructure de
patch pour Solaris*

Objectifs fixés

- Toute nouvelle installation/réinstallation doit être à jour
- A tout moment, les machines déjà installées doivent être à jour
- Tout changement sur une machine doit être opéré à distance
- Sécuriser les machines et les connexions
- Automatiser au maximum

Plateforme du labo

- **Linux RedHat**
 - Installation avec kickstart (rpm)
 - Administration avec cfengine
 - Mise à jour avec yum (updates)
 - Sécurisation (élimination de services, iptables)
- **Solaris**
 - Installation avec jumpstart (pkg)
 - Administration avec cfengine
 - Mise à jour avec PatchPro (patches)
 - Sécurisation (élimination de services, tcpwrappers)

C'est quoi un patch ?

- Une collection de fichiers et de répertoires
- Destiné à remplacer ou à mettre à jour des fichiers et des répertoires d'un software (pkg) déjà existant
- Etroitement lié à un package
- Identifié par un ID unique (ex: 113575-05) :
 - Un « base code » unique (en général sur 6 chiffres)
 - Un tiret
 - Un numéro de révision sur 2 chiffres

Quels sont les types de patches ?

- Standard patches : problèmes liés à l'OS, matériel, autres produits logiciels
- Recommended patches
- Security patches
- Y2K patches
- Patch clusters : patches groupés
- Point patches : patches personnalisés, fixer un problème unique
- Maintenance updates (MU) : ensemble de patches prétestés

Où trouve-t-on les patches ?

- Avec contrat SunSpectrum :
 - Tout type de patch
- Sans contrat :
 - Security patches
 - Recommended patches

sunsolve.sun.com (http, https, ftp)

Patches signés

- La signature permet de vérifier l'authenticité et l'intégrité d'un patch SUN
- Extension .jar (.zip pour les non signés)
- Solaris 2.6, 7, 8 et 9
- SUNWcert, keytool (voir README SUNWcert)
- Certificats SUN : <http://www.sun.com/pki/index.html>

La base SunSolve

- 19 Octobre 2003
- Nombre total de patches signés = 3159 (5 Go)
- Patches SunOS 5.6 à 5.9 = 1982

	Total	Security	%
SunOS 5.6	459	181	39.43
SunOS 5.7	441	160	36.28
SunOS 5.8	613	176	28.71
SunOS 5.9	307	83	27.03
SunOS 5.6_x86	230	136	59.13
SunOS 5.7_x86	210	116	55.24
SunOS 5.8_x86	280	117	41.78
SunOS 5.9_x86	84	43	51.19

Outils de gestion de patches

Gestion = analyse, installation/désinstallation

- patchadd/patchrm : commandes Unix (Patch Finder)
- PatchDiag Tool : uname, pkginfo, showrev, patchdiag.xref
- Patch check : +Perl, Rapports en HTML
- PatchPro Interactive : page web
- PatchPro Expert : applet signée
- Patch Manager (PatchPro)

Feature	patchadd and patchrm Commands	Patch Check	PatchPro Interactive or PatchPro Expert	Solaris 2.6, Solaris 7, and Solaris 8 Patch Management Tool	Solaris 9 Patch Management Tool
How do I get this tool?	Included in Solaris release (SUNWswmt)	SunSolve Online site	Run tool from PatchPro Web site	Download Solaris Patch Manager Base 1.0.1 from PatchPro Web site	Download PatchPro 2.2 from PatchPro Web site
Solaris release availability	Solaris 2.6, Solaris 7, Solaris 8, and Solaris 9	Solaris 2.6, Solaris 7, Solaris 8, and Solaris 9	Solaris 2.6, Solaris 7, Solaris 8, and Solaris 9	Solaris 2.6, Solaris 7, and Solaris 8	Solaris 9
Applies signed patches?	Yes	No	No	Yes, and automatically verifies the signed patch when it is downloaded	Yes, and automatically verifies the signed patch when it is downloaded
Applies unsigned patches?	Yes	Yes	No	No	Yes
GUI available?	No	No	No	No	Yes
Analyzes system for recommended patches, and downloads patches	No	Yes, unsigned patches only	Yes, unsigned patches only	Yes, signed patches only	Yes, signed patches only
Local and remote system patch support	Local	Local	No	Local	Local and remote
RBAC support?	No	No	No	No	Yes

Notre choix



- Patch Manager (PatchPro)
 - Permet l'analyse
 - Installe des patches signés

Et l'automatisation ?

- Analyse et installation :
 - smpatch (nécessite une authentification)
 - pprosvc
- Problèmes :
 - Dépendance entre patches
 - L'analyse est parfois en décalage par rapport à la base SunSolve
 - Certains patches sont « séquestrés »

Propriétés d'un patch

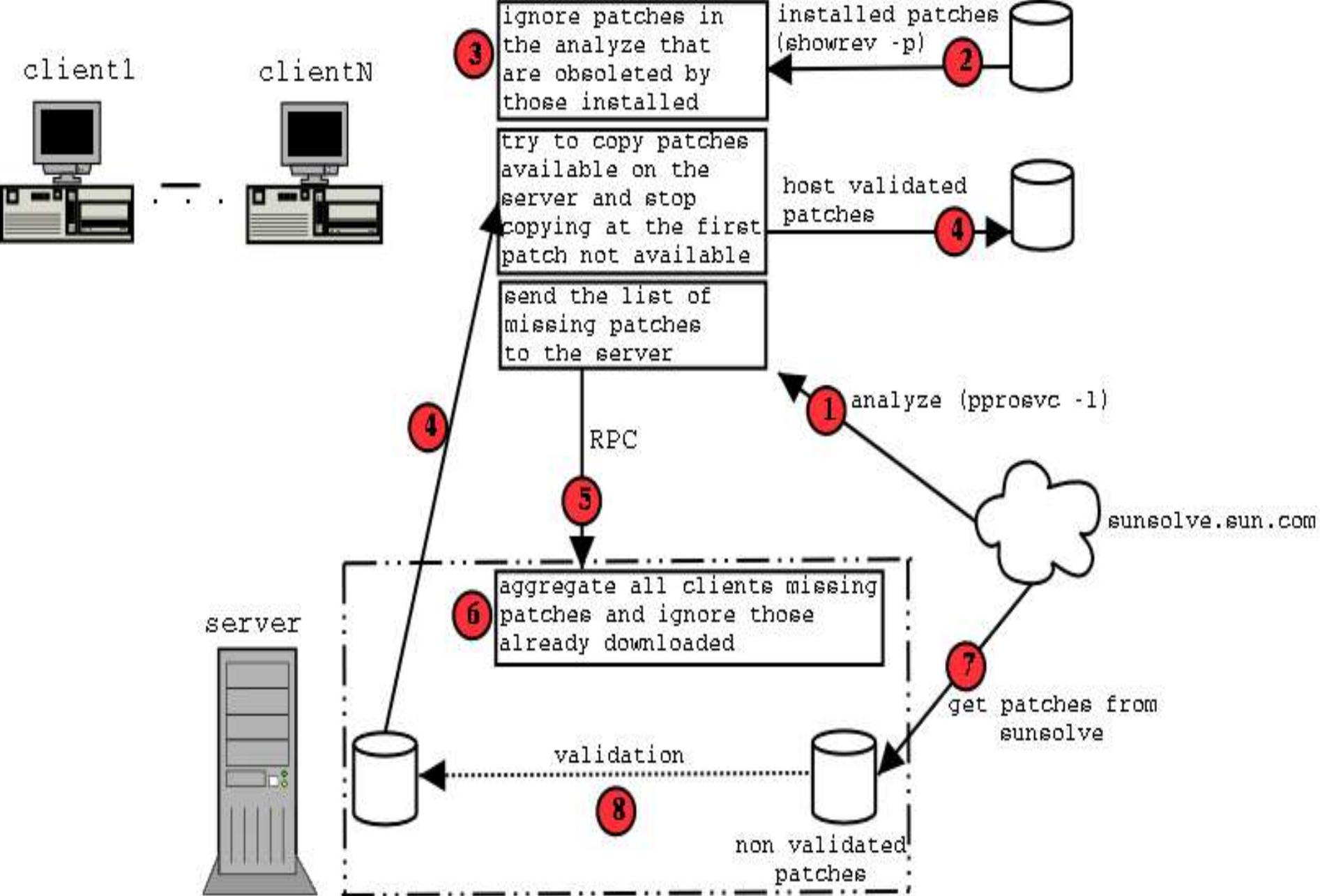
- obsolete, discontinued
- noncontract, clientroot, clientusr
- rebootimmediate, rebootafter, reconfigimmediate, reconfigafter
- interactive, pointpatch, nonstandard
- Singleuser

Quelques chiffres

	6	7	8	9	6_x86	7_x86	8_x86	9_x86
Clientroot	42	38	106	73	18	11	51	18
Clientusr	58	62	155	127	45	43	105	58
Interactive	43	44	96	25	14	17	36	5
Noncontract	10	10	15	14	0	0	0	0
Nonstandard	12	13	14	5	0	0	3	0
Pointpatch	0	0	3	0	0	0	2	0
Rebootafter	47	47	81	74	21	17	37	15
Rebootimmediate	6	6	10	17	2	3	3	2
Reconfigafter	1	1	18	5	1	1	4	1
Reconfigimmediate	0	0	11	5	0	0	4	1
Singleuser	17	15	34	35	8	6	10	9
Discontinued	0	0	0	0	0	0	0	0
Obsolete	0	0	0	0	0	0	0	0

Notre solution

- Clients : analyse effectuée sur SunSolve
- Serveur : « Patches repository » chez nous
- Tout est installé en single user mode
- Ptés : rebootafter, rebootimmediate, reconfigafter, reconfigimmediate, none (à partir de README.<ID> et patchinfo)
- Pré et post installation



Liens



- <http://sunsolve.sun.com>
- <http://docs.sun.com>